Rain Merimaa

Yrityksen asiakaspalvelupisteiden internetin käytön rajoittaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

18.9.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Rain Merimaa Yrityksen asiakaspalvelupisteiden internetin käytön rajoittaminen 27 sivua + 1 liite 18.9.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkkotekniikka
Ohjaaja	koulutuspäällikkö Markku Karhu

Insinöörityön tavoite oli suunnitella ja toteuttaa jokin menetelmä tai tapa, jonka avulla olisi mahdollista rajata yrityksen Pohjoismaissa sijaitsevien asiakaspalvelupisteiden Internetin käytön vain yrityksen sallimille sivustoille. Ennen tätä toteutusta yrityksen asiakaspalvelupisteiden tietokoneiden Internetin käytön rajoittamiseen ei ollut mitään helppoa ja keskitettyä tapaa.

Aluksi työssä käydään läpi yleisesti internetin käytön rajoittamista ja siinä käytettyjä tekniikoita, jotta lukija saisi paremman käsityksen aiheesta. Tämän jälkeen siirrytään käytännön työn pariin.

Yrityksellä on asiakaspalvelupisteitä Pohjoismaissa ja jokaisessa näissä on noin kymmenen työntekijää, joita rajoituksen tulisi koskettaa. Asiakaspalvelupisteillä on myös esimiehiä sekä tietokoneita, joita tämä rajoitus ei tulisi koskettaa. Toteutuksessa päädyttiin käyttämään Squid-nimistä välityspalvelinta ja välityspalvelimet asennettiin erikseen kaikkien asiakaspalvelupisteiden omalle paikalliselle palvelimelle. Toteutuksessa käytettiin avuksi myös Microsoftin ryhmäkäytäntöjä.

Lopputuloksena välityspalvelimet täyttivät annetut vaatimukset, joita olivat muun muassa keskitetyt pääsylistat ja esimiesten pääsy rajoituksen läpi. Koska käytettiin avoimen lähdekoodin ohjelmistoa, rahaa ei kulunut toteutukseen. Toteutus onnistui hyvin ja se on käytössä tällä hetkellä ja sitä tullaan ylläpitämään ja kehittämään jatkossakin.

Avainsanat	Squid, välityspalvelin, internetin käytön rajoittaminen

Author(s) Title Number of Pages Date	Rain Merimaa Restricting internet access at customer service locations 27 pages + 1 appendix 18 September 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Markku Karhu, Head of Degree Programme

The purpose of the project described in this bachelor's thesis was to find and create a way to restrict employees' internet access at the Northern European customer service locations of the target company and to allow the employees access to company approved websites only. Prior to this project there was no centralized and functional way to manage internet access at these locations.

The thesis describes how internet access can be restricted and the different techniques used to give the reader a better understanding of the subject. The main focus of the thesis is, however, the actual application implemented in the company.

To begin with, the company has customer service locations in the Nordic countries and about ten employees at each location whose internet access should be restricted. At the same time there are also managers and computers at these locations that should be exempt from these restrictions. In practice, the project was executed by using the Squid web proxy and installing the web proxy to all of the local servers of the customer service points. In addition, Microsoft group policies were used in the execution of the project.

The project was a success and all requirements were met. For example, the requirements included a centralized access control list and managerial exceptions. No money was spent on the project because open source codes were used. The web proxies are still in use at the company and will be maintained and improved.

Keywords	Squid, proxy, internet access restrictions

Sisällys

Lyhenteet

ACL	*Access Control List*, pääsylista. Lista säännöistä, joilla sallitaan tai estetään pääsy.
AD	*Active Directory*, aktiivihakemisto. Microsoftin käyttämä käyttäjätietokanta ja hakemistopalvelu.
DNS	*Domain Name System*, nimipalvelu. Nimipalvelun tehtävä on muuntaa verkkotunnukset IP-osoitteiksi.
FTP	*File Transfer Protocol*. Tiedonsiirtoprotokolla.
GPO	*Group Policy Object*, ryhmäkäytäntöobjekti. Koostuu yhdestä tai useasta ryhmäkäytännöstä.
HTTP	*Hypertext Transfer Protocol*. Tiedonsiirtoprotokolla, jota käytetään selaimen ja WWW-palvelimen väliseen tiedonsiirtoon.
HTTPS	*Hypertext Transfer Protocol Secure*. HTTP-protokolla, johon on lisätty tiedon salaus.
MPLS	*Multiprotocol Label Switching*. Isoihin verkkoihin tarkoitettu IP-pakettien kuljetusmenetelmä.
NTML	*NT LAN Manager*. Microsoftin todennusprotokolla.
SSL	*Secure Sockets Layer*. Salausprotokolla, jota käytetään mm. HTTPS-liikenteessä.
VPN	*Virtual Private Network.* Mahdollistaa verkkojen ja tietokoneiden liittämisen samaan verkkoon internetin välityksellä.

1 Johdanto

Nykypäivänä internetin käyttöä rajoitetaan sekä sensuroidaan yllättävän paljon. Esimerkiksi Suomen viranomaisten määräyksestä palveluntarjoajat Suomessa ovat joutuneet sensuroimaan muun muassa lain vastaisia sivustoja pois käyttäjien ulottuvilta. Kouluissa estetään sivustoja, joissa ei haluta oppilaiden käyvän oppituntien aikana tai kotona oman lapsen pääsyn estäminen tietyille sivustoille.

Insinöörityöraportissa käydään läpi internetin käytön rajoituksen suunnittelu ja toteutus alusta alkaen yrityksen tarpeisiin. Työ tuli toimeksiantona työsuhteen aikana, ja sen suunnittelu ja toteutus oli kokonaisuudessaan minun vastuullani. Tavoitteena oli saada helposti ja keskitetysti hallittava esto, jonka päätarkoituksena olisi rajoittaa internetin käyttö ainoastaan sallituille sivustoille sekä ottaa huomioon esimiehet ja sallitut tietokoneet.

Työ lähti liikkeelle sopivan toteutustavan etsimisellä, ja aluksi tuli pohtia eri vaihtoehtoja, esimerkiksi, tulisiko työ toteuttaa ohjelmallisella rajoituksella, välityspalvelimella tai muulla tavalla jolla internetin käyttöä olisi mahdollista rajoittaa. Valitun toteutustavan tulisi täyttää annetut vaatimukset, joita olivat muun muassa helppo ylläpitäminen ja käyttäjien todentaminen.

2 Internetin käytön rajoittaminen

Internetin käyttöä voidaan rajoittaa ja sensuroida hyvin monella toisistaan erilaisella menetelmällä. Seuraavaksi käydään lyhyesti läpi yleisimpiä menetelmiä ja toteutustapoja.

2.1 Välityspalvelin

Yleisimpiä tapoja rajoittaa internetin käyttöä on hyödyntää välityspalvelinta. Välityspalvelimella voi olla myös paljon muitakin tehtäviä. Sitä voidaan käyttää esimerkiksi välimuistina Internet-liikenteelle, suojaamaan omaa yksityisyyttä tai seuraamaan, millä sivustoilla käyttäjät käy.

Määritetty sekä läpinäkyvä välityspalvelin

Välityspalvelimen käyttöönottotavoista yleisimmät ovat määritelty välityspalvelin sekä läpinäkyvä välityspalvelin. Määritellyssä välityspalvelimessa on määritettävä käyttäjälle välityspalvelin käyttöön. Tämä voi olla esimerkiksi selaimen asetuksiin tehtävä asetus. Kotikäyttäjä voi esimerkiksi ottaa omaan selaimeen käyttöön toisessa maassa sijaitsevan julkisen välityspalvelimen, jolloin Internet-liikenne menee toisen maan kautta ja täten sivustot luulevat, että käyttäjä surffailee maassa, jossa välityspalvelin sijaitsee. Näin voidaan kiertää muun muassa maakohtaisia rajoituksia eri internet-sivustoilla.

Läpinäkyvää välityspalvelinta käytetään usein työpaikoilla ja kouluissa. Tällöin käyttäjien koneille ei ole tarvetta tehdä mitään asetuksia vaan kaikki liikenne, mikä menee verkosta ulospäin, menee automaattisesti välityspalvelimen läpi. Tällöin käyttäjät eivät voi kiertää välityspalvelinta eivätkä välttämättä edes tiedä liikenteensä menevän välityspalvelimen kautta.

Välityspalvelinohjelmistot

Internetin käytön rajoittamiseen soveltuvia välityspalvelinratkaisuja ja ohjelmistoja on useita. Isoissa yrityksissä, joissa käytetään Microsoftin tuotteita, on usein myös käytössä Microsoftin FTMG (Forefront Threat Management Gateway), joka tarjoaa ja hoitaa

monia rooleja verkossa. Se voi toimia myös välityspalvelimena, ja siihen haluttujen estettävien sivustojen lisäys on hyvin yksinkertaista graafisen ympäristön avulla.

Suosituimpia avoimen lähdekoodin välityspalvelimia, joilla onnistuu sivustojen rajoittaminen, ovat Squid ja Privoxy. Squid on monipuolinen välityspalvelin, ja sillä onnistuu muun muassa käyttäjien todennus, verkkoliikenteen analysointi ja suodatus sekä nimipalvelun ja Internet-liikenteen välimuistissa pitäminen. Privoxy on taas huomattavasti yksinkertaisempi, ja siinä on vähemmän ominaisuuksia. Se keskittyykin pääasiassa mainosten estoon mutta sillä on helppo toteuttaa erilaisia rajoituslistoja, kuten listoja sallituista tai estetyistä sivustoista.

2.2 DNS- ja IP-esto

DNS (*Domain Name System*) -eston toteuttaminen tapahtuu niin, että nimipalvelimelta estetään tai uudelleenohjataan osoite tai osoitteet, joihin ei haluta käyttäjien saavan yhteyttä. DNS-rajoitus on kuitenkin hyvin helppo kiertää vaihtamalla oman laitteen tai tietokoneen käyttämää nimipalvelinta. Sen takia lisätään myös estettyjen osoitteiden IP-osoitteet palomuurin estolistalle. Tätä tapaa käyttävät muun muassa Elisa ja Sonera niin sanotussa Piratebay-estossa. [10,11.]

2.3 Ohjelmallinen toteutus

Kotona esimerkiksi lapselle rajoituksen toteuttaminen on kaikkein helpointa asentamalla tietokoneelle ohjelma, jolla onnistuu rajoituksen luominen. Ohjelmissa voi usein valita estettäviä sivustoja ja valita esimerkiksi estoon kaikki sivustot, jotka sisältävät tiettyjä sanoja. Näin voi helposti esimerkiksi aikuisviihteeseen viittaavat sivut saada helposti pois lapsen ulottuvilta. Käteviä ohjelmia tähän tarkoitukseen ovat muun muassa F-Securen Internet Securityn mukana tuleva lapsilukko. Ilmaisia vaihtoehtoja on myös hyvin paljon ja esimerkiksi Microsoftin Essentials -paketti sisältää Perheturva-nimisen apuohjelman, jolla voi hyvin monipuolisesti rajoittaa internetin käyttöä. [12.]

3 Työn toteutus

Tehtävänanto toteuttaa internetin rajoittaminen asiakaspalvelupisteisiin tuli seurauksena asiakaspalvelupisteiden ryhmänjohtajien palavereista. Rajoituksen tarkoitus on rajata Internet-sivustot sellaisiin sivustoihin, joita käytetään työssä tai joista on apua työntekijöille.

Jokaisessa asiakaspalvelupisteessä on myös toimistokone, jota rajoitus ei tulisi koskemaan. Tällä tietokoneella työntekijät voivat käyttää internetiä vapaasti esimerkiksi taukojen aikana tai työajan ulkopuolella. Rajoitus ei myöskään saisi koskea esimiehiä, eli rajoituksen toteutuksessa tulisi myös ottaa esimiehet huomioon.

Yrityksellä on asiakaspalvelupisteitä yhteensä kuusi kappaletta ympäri Pohjoismaita, Islantia lukuun ottamatta. Kolme niistä sijaitsee Suomessa ja loput Norjassa, Ruotsissa ja Tanskassa. Lähiaikoina Suomeen on tulossa vielä yksi asiakaspalvelupiste, joka myös tullaan lisäämään rajoituksen piiriin.

Toteutukselle asetettiin seuraavanlaiset vaatimukset:

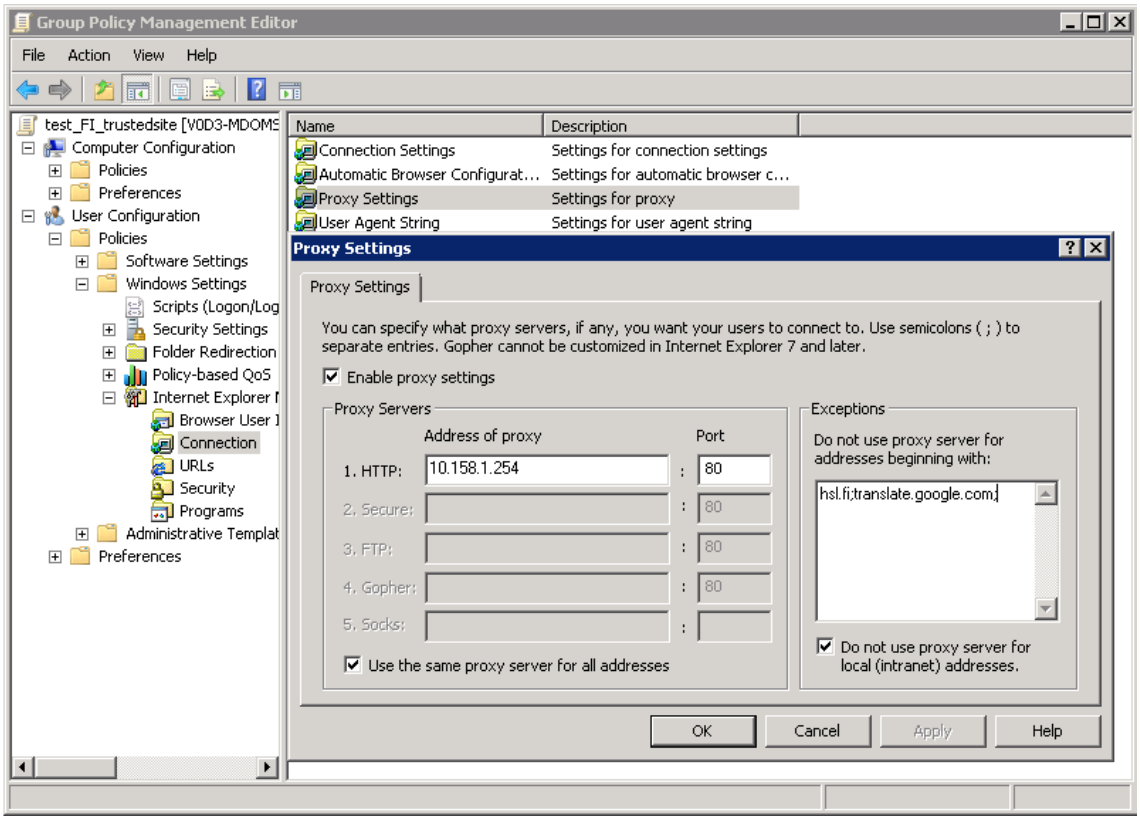
- Pääsy ainoastaan sallittuihin sivustoihin, eli niin sanottu "whitelist"-menetelmä.
- Helppo ja keskitetty hallinta.
- Rajoituksen ei tulisi koskettaa esimiehiä eikä toimistokoneita.
- Yhtenäinen sallittujen sivujen lista, joka päivittyy kaikkiin asiakaspalvelupisteisiin.

Vaatimukset huomioon ottaen jouduttiin pohtimaan erilaisia vaihtoehtoja työn toteutukselle. Niitä olivat muun muassa ohjelmallinen toteutus, Internet Explorer -asetuksien muuttaminen Group Policyn avulla sekä välityspalvelin.

Ohjelmallisessa toteutuksessa olisi asennettu tietokoneille asiakasohjelman, joka rajoittaa tietokoneen internetin käyttöä. Tällaisen toteutuksen toteuttamiseen ei kuitenkaan lähdetty, koska asetettujen vaatimusten täyttäminen olisi hyvin epätodennäköistä.

Internet Explorer -asetuksien muuttaminen ryhmäkäytännöillä *(Group Policies)* mahdollistaisi keskitetyn hallinnan. Toteutustapoja, joissa tätä voisi hyödyntää, on parikin kap-

paletta. Voitaisiin esimerkiksi luoda ryhmäkäytäntö, joka koskisi ennalta määritettyjä työntekijöitä. Ryhmäkäytäntöön olisi määritetty, että kaikki HTTP-liikenne menisi välityspalvelimelle, jota todellisuudessa ei olisi olemassa. Samalla määritettäisiin sivut, jotka ohittaisivat tämän keksityn välityspalvelimen, eli sivut määritettäisiin Exceptions-listaan (ks. kuva 1). Kun selain hakee HTTP-sivua, jota ei ole määritetty Exceptions-listaan, selain lähettää sivun latauspyynnön välityspalvelimelle, jota ei ole olemassa, eli vastausta ei tule takaisin eikä käyttäjä saa hakemaansa sivustoa. Kun taas selain hakee sivua joka, on määritetty Exceptions-listaan, selain ei lähettäisikään pyyntöä välityspalvelimelle Sen sijaan se lähetetään oletusyhdyskäytävään, joten sivu aukeaa käyttäjälle. Tätä tapaa ei kuitenkaan lähdetty kokeilemaan testiympäristön ulkopuolelle.



Kuva 1. Välityspalvelimen määrittäminen ryhmäkäytännöllä.

Työn toteutuksessa päädyttiin käyttämään omaa hallittavaa välityspalvelinta. Vaikka aluksi tämän vaihtoehdon toteutus tuntuikin monimutkaiselta, se vaikutti kuitenkin olevan ainoa järkevä ja oikeaoppinen tapa toteuttaa rajoitus asiakaspalvelupisteisiin. Aluksi työ lähtikin liikkeelle sopivan välityspalvelinohjelmiston löytämisellä. Koska tarkoitus oli toteuttaa ratkaisu ilman kustannuksia, lähdettiin liikkeelle avoimen lähdekoo-

din ohjelmista. Avoimen lähdekoodin välityspalvelimista löytyikin muutama varteenotettava ja suosittu vaihtoehto, joita lähdettiin miettimään.

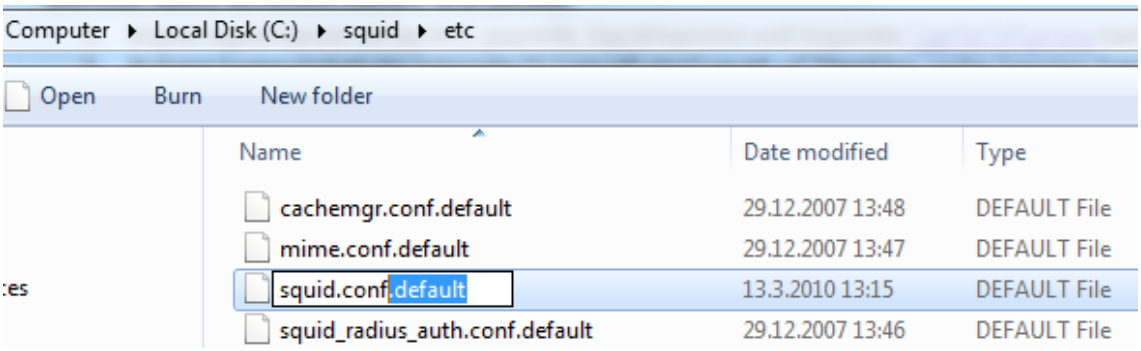
Avoimen lähdekoodin välityspalvelimista Squid sekä Privoxy vaikuttivat olevan varteenotettavia vaihtoehtoja. Ne myös vaikuttivat olevan kaikkein suosituimpia juuri sellaisten vaatimusten täyttämiseen, joita tässä työssä haettiin. Molemmista ohjelmistoista löytyy niin Windows- kuin myös Linux-versio. Työssä päädyttiin kuitenkin käyttämään Squid-välityspalvelinta, koska se tukee muun muassa käyttäjien todennusta, joka on tärkeä osa työn toteutuksessa.

Aluksi lähdin toteuttamaan Squid-asennusta Linux-ympäristöön, mutta siirryin Windows-version pariin tajuttuani, että olisi liian työlästä asentaa virtuaalista Linux-palvelimia jokaisen asiakaspalvelupisteen Windows-palvelimeen.

Välityspalvelimen kanssa kuitenkin kävi mielessä, että ongelmia saattaa tulla yhteisen sallittujen sivustojen listan toteuttamisessa ja päivittämisessä, koska tarkoitus olisi kuitenkin asentaa jokaiseen palvelupisteeseen oma välityspalvelin, jolla on omat asetukset. Kuitenkin niillä kaikilla tulisi olla yhteinen sallittujen sivujen lista helppokäyttöisyyden takaamiseksi.

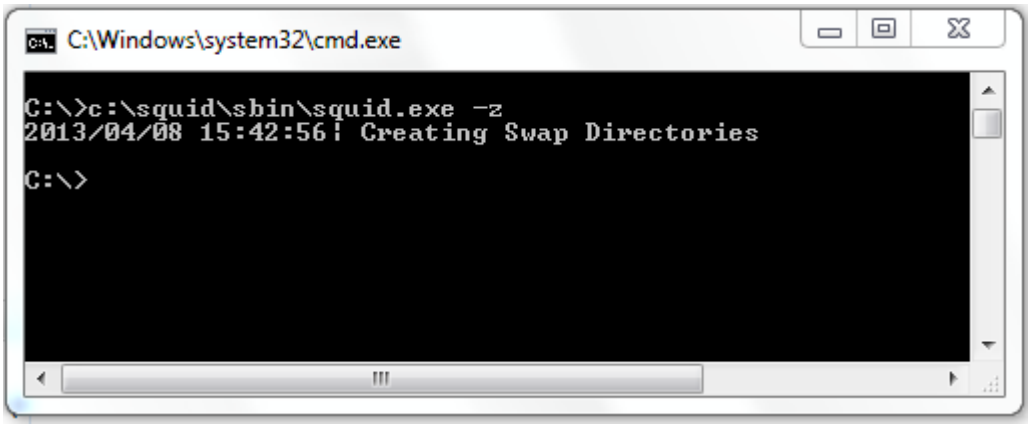
3.1 Squidin asennus ja käyttöönotto testiympäristössä

Squidin asennus lähti liikkeelle Squidin Windows-asennuspaketin hakemisella. Squid versioksi valittiin 2.7STABLE8, koska se on viimeisin vakaa Windowsille käännetty versio. Kun asennuspaketti oli ladattu, se purettiin .zip -tiedostosta, jonka jälkeen siitä tuleva Squid-niminen kansio siirrettiin Windowsin C:\ -aseman juureen. Tämän jälkeen tuli tehdä tarvittavat toimenpiteet, jotta Squidin saisi käyntiin. Aluksi poistettiin .default-pääte c:\squid\etc\ -kansiosta löytyvien konfiguraatiotiedostojen päätteestä (ks. kuva 2). Jos tätä ei tehnyt, niin Squidin käynnistyksen yhteydessä tuli virhesanoma, että konfiguraatiotiedostoja ei löydy.



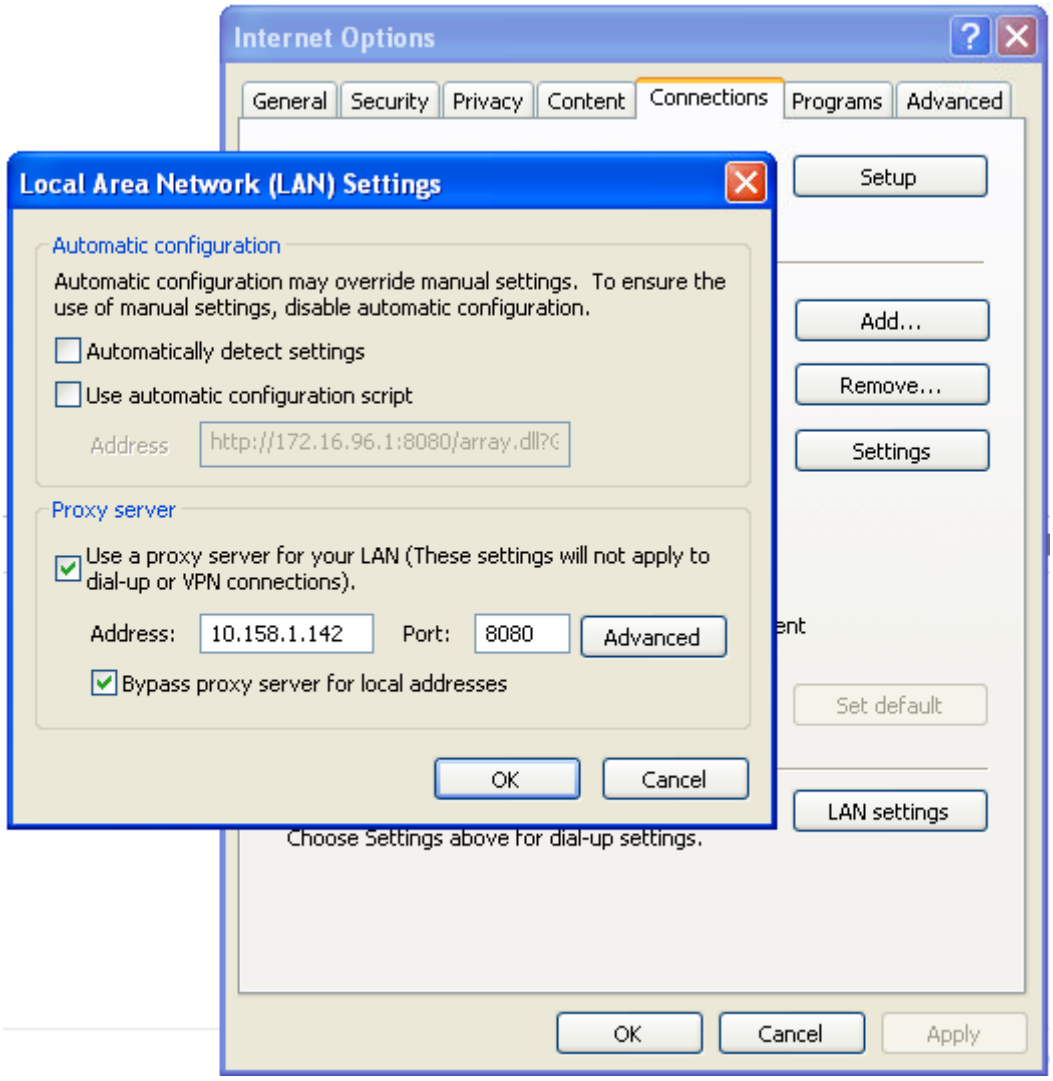
Kuva 2. Konfiguraatiotiedostojen .default -päätteet.

Tämän jälkeen oli luotava Squidin välimuistin käyttöä varten sille tarvittavat kansiot. Tämä tapahtui käynnistämällä Squid "-z" -parametrilla, eli Windowsin komentokehote tuli tehdä auki ja siihen kirjoittaa "c:\squid\sbin\squid.exe -z" (ks. kuva 3).



Kuva 3. Squidin välimuistikansioiden luominen.

Komennon jälkeen c:\squid\var-kansioon ilmestyi cache-niminen kansio, jota Squid käyttää välimuistin säilyttämiseen. Kun edelliset toimenpiteet oli tehty oikein, Squid käynnistyi onnistuneesti, kun ajettiin komentokehotteessa "c:\squid\sbin\squid.exe" -komento. Tämän jälkeen asetettiin toinen testikone käyttämään äsken käynnistettyä Squid-välityspalvelinta. Tämä tapahtui muuttamalla Internet Explorerin asetuksia. Internet Explorerin asetuksissa on Connections-niminen välilehti, josta valittiin kohta "LAN settings", ja sieltä pystyttiin asettamaan Squid-välityspalvelin käyttöön (ks. kuva 4). Address-kohtaan tuli laittaa sen testikoneen IP-osoite, johon Squid oli asennettu. Port: -kohtaan laitettiin 3128, koska se on portti, jota Squid kuuntelee oletusasetuksilla.



Kuva 4. Internet Exploreriin välityspalvelimen käyttöönottaminen.

Seuraavissa luvuissa perehdytään tarkemmin konfiguraatio tiedostojen muokkaamisen yritykselle soveltuvaksi. Nykyisestä oletuskonfiguraatiosta on hyvä ottaa kopio talteen ja tämän jälkeen luotiin täysin tyhjä konfiguraatiotiedosto, jotta siitä saisi mahdollisimman yksinkertaisen ja selkeän. Alkuperäinen konfiguraatio kannattaa pitää tallessa, koska se toimii hyvänä esimerkkinä ja siinä on selitetty eri parametrien tarkoituksia.

3.1.1 Todentaminen

Työssä tarvittiin jonkinlainen käyttäjien todennusmenetelmä. Välityspalvelimen tuli tunnistaa esimiehet muiden joukosta, koska esimiehillä tuli olla oikeus päästä kaikille sivustoille kaikilta tietokoneilta. Koska kaikki käyttäjät ovat aktiivihakemistossa *(Active*

Directory) ja he kirjautuvat tietokoneille omilla tunnuksilla, on täten tietokanta käyttäjistä jo olemassa.

Squid tukee kaikkia neljää merkittävintä todennusmenetelmää. Niitä ovat Basic, NTML, Digest sekä Negotiate. Koska Squid asennettiin Windows-tietokoneeseen, joka on jo liitetty aktiivihakemistoon, on todentamisen lisääminen yksinkertaista Squidin konfiguraatioon. Jos kyseessä olisi esimerkiksi Linux-tietokone, jossa pitäisi saada todentaminen aktiivihakemistoon toimimaan, vaatisi se huomattavasti enemmän työtä. Tässä tapauksessa kuitenkin riittää vain muutama rivi tekstiä. Päädyin käyttämään NTML-todennusmenetelmää, vaikkakin Negotiate eli Kerberos on NTML:n korvaaja. NTML on kuitenkin paremmin tuettuna varsinkin vanhemmissa järjestelmissä.

Todentamista Squidissa käytetään pääsääntöisesti siihen, että estetään todentamattomien käyttäjien pääsy esimerkiksi intranetiin tai internetiin. Tässä työssä sitä kuitenkin käytettiin vain esimiesten todentamiseen, koska yrityksellä ei ole tarvetta estää pääsyä todentamattomilta käyttäjiltä. Lisätään uuteen tyhjään konfiguraatiotiedostoon seuraavat rivit:

```
auth_param ntlm program c:/squid/libexec/mswin_ntlm_auth.exe
auth_param ntlm children 20
```

Ensimmäisellä rivillä määritetään Squidin apuohjelman polku, joka hoitaa NTML-todennusta. Toisella rivillä määritetään, montako todentamisprosessia voi olla samanaikaisesti auki. Jos tämä arvo olisi esimerkiksi yksi, niin vain yksi todentaminen voi tapahtua kerralla ja seuraava menee jonoon, mikä hidastaa seuraavan käyttäjän todentamisprosessia. Arvo kannattaa laittaa suureksi varsinkin silloin, jos yhteys todennuspalvelimelle on hidas.

Nykypäivänä kaikki verkkoselaimet tukevat NTML-todennusta, joten käyttäjän todentaminen tapahtuukin Windowsiin kirjautuessa. Selaimet osaavat suoraan hyödyntää jo kertaalleen todennettua käyttäjää. Jos kuitenkin käyttäjällä on käytössä useita vuosia vanha versio esimeriksi Opera-verkkoselaimesta tai Google Chromesta, saattavat he joutua tekemään todennuksen selaimen käynnistettyä.

3.1.2 Pääsylistat

Pääsylistat ovat erittäin oleellinen osa Squidin konfiguraatiota. Pääsylistat ovat nimensä mukaisesti listoja, joille määritetään pääsy tai esto. Pääsylistat alkavat aina lyhenteellä ACL, joka on lyhenne sanoista Access Control List. Sen perään määritetään pääsylistan nimi, jonka jälkeen pääsylistan tyyppi ja lopuksi sen sisältö. Jos sisältöön tulee esimerkiksi kaksi tietokoneen IP-osoitetta, voidaan ne erotella välilyönnillä. Välillä on tarvetta syöttää pääsylistan sisältöön esimerkiksi koko aliverkko, tällöin voidaan IP-osoitteen perään määrittää aliverkon maskin. Myös esimerkiksi tekstitiedoston sisältö voidaan määrittää pääsylistan sisällöksi, silloin sisältö on erotettava rivinvaihdolla toisistaan tekstitiedoston sisällä. [6.]

Taulukko 1. Yleisimpiä pääsylistan tyyppejä.

Pääsylistan tyyppi	**Käyttötarkoitus**
src	lähteen IP osoiteet
dst	kohteen IP osoiteet
srcdomain	lähteen toimialue
dstdomain	kohteen toimialue
time	kellonajalle ja/tai päiville
arp	MAC-osoitteille
port	kohteen porttinumero
proto	protokolla tyyppi

Taulukosta 1 saa käsityksen, minkä tyyppisiä pääsylistat voivat olla. Pääsylista tyyppejä on Squidissa yli kolmekymmentä erilaista. Seuraavaksi määritettiin tarvittavat pääsylistat konfiguraatioon ja lisättiin kommenttirivit, jotta myöhemminkin muistaisi, mitä pääsylistat pitävät sisällään.

```
#Sisältää koko verkon
acl all src 0.0.0.0/0.0.0.0

#Sisältää listan sallituista verkkotunnuksista
acl whitelist dstdomain "c:\squid\etc\whitelist.txt"
#Sisältää listan sallituista tietokoneista
acl koneet src "c:\squid\etc\sallitutkoneet.txt"
#Sisältää sallitut käyttäjät (esimiehet, IT)
acl esimiehet proxy_auth "c:\squid\etc\esimiehet.txt"
```

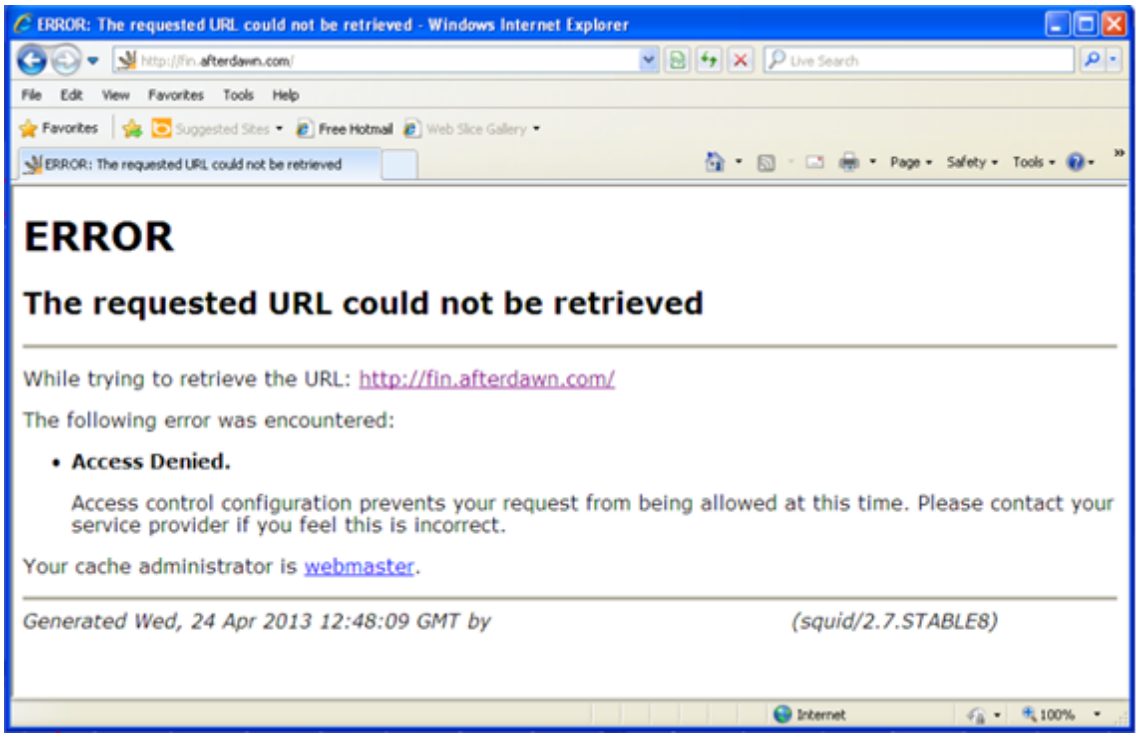
```
#Sisältää avoimet portit
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl SSL_ports port 443

#Sisältää FTP liikenteen
acl ftp proto FTP

#Käytetään tunnelointiin
acl CONNECT method CONNECT
```

Kuten konfiguraatiossa näkyy, työssä käytettiin kolmea tekstitiedostoa pääsylisoille, joissa määritettiin sallitut sivustot ja tietokoneet sekä käyttäjät, joita rajoitus ei koske.

Pääsylistat "Safe_ports" ja "SSL_ports" sisältävät porttinumerot muun muassa seuraaville protokollille: HTTPS, HTTP, FTP, SSL ja WAIS. Nämä ovat oletuksena määritetty avoimiksi porteiksi Squidin oletuskonfiguraatiossa.

3.1.3 Säännöt pääsylistoille

Kuten pääsylistoilla, myös pääsylistojen säännöillä on erilaisia tyyppejä. Oleellisin sääntötyyppi on kuitenkin http_access, jolla voidaan määrittää HTTP-pääsy, esimerkiksi sallitaanko tietyille käyttäjille tai tietokoneille pääsy internetiin. Kuvassa 5 näkyy virhesanoma, joka ilmestyy, kun sivustolle ei ole myönnetty pääsyä. Pääsylistan säännössä joko sallitaan *(allow)* tai estetään *(deny)* pääsy. Sääntö koostuu sääntötyypistä, säännöstä ja pääsylistasta. Esimerkiksi "http_access allow paasylista1" sallii HTTP-liikenteen "paasylista1" -nimiselle pääsylistalle, joka voisi sisältää esimerkiksi tietokoneita tai käyttäjiä. [6.]



Kuva 5. Estetty pääsy.

Squid käy pääsylistasäännöstöä järjestyksessä ylhäältä alas. Kun pääsylistan sisältö täsmää, ensimmäisen osuman sääntöä noudatetaan ja säännöstöjen läpikäynti lopetetaan. Tämän takia listan viimeiseksi kannattaakin aina laittaa "http_access deny all". Hyvä ajattelutapa onkin, että mitä ei sallita, se estetään. Säännöissä voidaan käyttää AND -operaatiota. Se voidaan toteuttaa laittamalla säännön perään kaksi tai useampia pääsylistoja. OR -operaation voidaan toteuttaa, kun laitetaan säännöt eri riveille. Pääsylistoille voidaan käyttää myös NOT -operaatiota, mikä onnistuu laittamalla huutomerkki pääsylistan eteen. Seuraavassa on esimerkit näiden hyödyntämisestä:

```
acl tyoaika time MTWHF 08:00-16:00
acl tyontekija kimmo pekka saara
acl toimistokone 192.168.0.6
http_access allow tyoaika tyontekijat
http_access deny all
```

Edellisessä esimerkissä työntekijät voivat käyttää internetiä vain työaikana.

```
acl tyoaika time MTWHF 08:00-16:00
acl tyontekija kimmo pekka saara
acl toimistokone 192.168.0.6
http_access allow tyontekija !time toimistokone
http_access deny all
```

Edellisessä esimerkissä työntekijät voivat käyttää toimistotietokonetta vapaasti työnajan ulkopuolella.

Seuraavaksi lisättiin säännöt työn tämänhetkisille konfiguraatio-tiedostoon. Merkitsin rivinumerot, jotta myöhäisemmässä vaiheessa voidaan tarkastella rivejä tarkemmin.

```
1 #Sallitaan käänteisesti yhteyden luomisen kaikkiin portteihin
2 http_access deny !Safe_ports
3 http_access deny CONNECT !SSL_ports
4 #Sallitaan FTP liikenne välityspalvelimen kautta
5 http_access allow ftp
6 #Sallitaan sallitut sivostot
7 http_access allow whitelist
8 #Sallitaan sallitut tietokoneet joita rajoitus ei koske
9 http_access allow koneet
10 #Sallitaan esimiehet ja IT:n
11 http_access allow kayttajat
12 #Estetään pääsy kaikelta mille ei ole määritetty pääsyä
13 http_access deny all
```

Jotta ymmärretään paremmin edellisen säännöstön toimintaperiaatteen, otetaan esimerkkitapauksia toiminnan havainnollistamiseksi (ks. taulukko 2).

Taulukko 2. Esimerkkitapaukset pääsylistasta.

Esimerkkitapaus / selitys	Rivi jossa ehto täsmää	Lopputulos
Työntekijä menee sivustolle jota ei ole sallittujen joukossa	13	Sivusto täsmää vasta viimeisellä rivillä olevaan "all" pääsylistaan, joten pääsyä ei anneta ja käyttäjä ei päästetä sivustolle
Esimies menee sivustolle jota ei ole sallittujen sivujen joukossa	11	Esimies on "kayttajat" listassa, joten pääsy sallitaan sivustolle
Esimies menee sallitulle sivustolle	7	Koska pääsy sallitaan sivustolle, ei ole enää tarvetta mennä listaa alaspäin.
Työntekijä menee toimistokoneella sivustolle jota ei ole sallittujen joukossa	9	Toimistokone on "koneet" pääsylistassa.
Esimies yrittää päästä HTTPS-sivustolle joka ottaa yhteyden porttiin 557	3	Kyseessä on HTTPS-sivu mutta kyseinen 557-portti ei ole sallittujen porttien joukossa, joten sivustolle ei pääse. Huomatkaa porttien käänteinen määrittelytapa. Näin estetään kaikki portit, poislukien määritettyjä

3.1.4 Pyyntöjen välittäminen eteenpäin

Muutamassa asiakaspalvelupisteessä ei ole suoraa ulospääsyä internetiin. Näissä palvelupisteissä tietokoneiden liikenne on ohjattu toiselle välityspalvelimelle. Näin ollen Squid on asetettava ohjaamaan pyynnöt eteenpäin toiselle välityspalvelimelle. Jotta tämä onnistuisi, lisättiin Squidin konfiguraatioon seuraavanlaiset rivit.

```
#cache_peer hostname type http-port icp-port [options]
cache_peer 172.16.5.1 parent 8080 0 no-query no-digest
never_direct allow all
```

Squid määritettiin niin, että se lähettäisi aina pyynnöt toiselle välityspalvelimelle. Squidin ohjaama liikenne lähetetään IP-osoitteeseen 172.16.5.1 ja porttiin 8080, jota toinen välityspalvelin kuuntelee. ICP-porttia käytetään välityspalvelinten välimuistin hyödyntämiseen, mutta koska toinen välityspalvelin ei kerää välimuistia, asetettiin arvon nollaksi sekä laitettiin no-query- sekä no-digest-asetukset päälle, jolloin Squid ei lähetä ICP-pyyntöjä eikä Cache Digest -pyyntöjä. Välityspalvelimen tyypiksi asetettiin "parent" tyypin, joka tarkoittaa sitä, että kun välityspalvelimella ei ole välimuistissa haluttua tietoa, välittää se pyynnön eteenpäin. Tässä tapauksessa välityspalvelin aina välittää

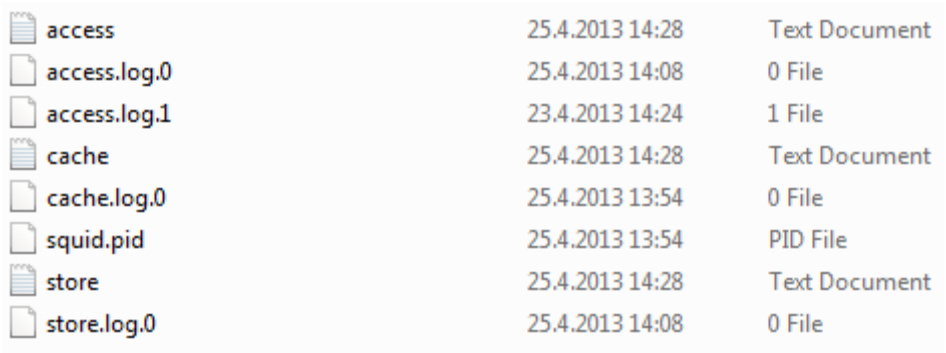
pyynnön eteenpäin. Viimeisellä rivillä oleva "never_direct allow all" tarkoittaa, että mitään pyyntöä ei lähetetä suoraan kohteeseensa, vaan ne menevät määritetyn välityspalvelimen kautta. [7.]

3.1.5 Lokitiedostot

Lokitiedostot ovat tärkeitä tiedonlähteitä Squidin toiminnan ja vianetsinnän kannalta. Oletuksena Squid tallentaa tietoa kolmeen eri lokitiedostoon:

- access.logiin tallennetaan tiedot HTTP pyynnöistä.
- cache.logiin tallennetaan Squidin toiminnan kannalta tärkeää tietoa.
- store.logiin tallennetaan kaikki tieto kirjoitetusta ja poistetusta välimuistista.

Lokitiedostot voidaan ottaa pois käytöstä, mutta sitä ei suositella, koska vian tai ongelman sattuessa ei ole mitään, mistä vikaa voisi lähteä etsimään. Lokitiedostojen haittapuolena on se, että ne voivat paisua erittäin suuriksi ja tällöin vievät kiintolevytilaa huomattavia määriä. Lokitiedostoja ei pystytä suoraan poistamaan, vaan lokitiedostot tulee "pyöräyttää" ympäri. Tällöin Squid lisää nykyisen lokitiedoston perään päätteen ".0" ja tämän jälkeen vapauttaa ne ja luo uudet tyhjät lokitiedostot, kuten kuvassa 6 näkyy. Nämä vapautetut lokitiedostot pystytään vapaasti poistamaan tai siirtämään. Kun käytössä olevia lokitiedostoja yrittää poistaa, tulee virheilmoitus, että ne ovat käytössä.



Kuva 6. Kuva pyöritetyistä lokitiedostoista.

Lokitiedostot voidaan pyöräyttää suorittamalla komentokehotteessa komento "c:\squid\sbin\squid.exe -n squid -k rotate".

Squid tallentaa access.log- sekä store.log- lokitiedostojen aikaleimat Unix-aika- muodossa. Unix-aika ilmaisee ajan sekunteina ajanhetkestä 1.1.1970. Esimerkiksi 12.3.2013 kello 16:00 on unix-aika- muodossa ilmaistuna 1363104000, joka ei siis ole kovin havainnollistava. Vianetsinnän takia on kuitenkin tutkittava access.log lokitiedostoa ja jotta nähtäisiin aika ymmärrettävässä muodossa, lisättiin Squidin konfiguraatioon seuraavanlaiset rivi:

```
logformat squid %tl.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log c:/squid/var/logs/access.log squid
```

Näin luotiin Squidiin uusi lokiformaatti. Tämä lokiformaatti muuttaa aikaleimat ymmärrettävään muotoon. Viimeisellä rivillä otetaan "squid" -niminen lokiformaatti käyttöön access.log -lokiin.

3.1.6 Konfiguraation viimeisteleminen

Jotta päästiin kokeilemaan luotua konfiguraatiota, jouduttiin vielä asettamaan portti, jota Squid kuuntelee. Oletuskonfiguraatiossa tämä on määritetty porttiin 3128, mutta se määritettiin helpommin muistettavaan 8080-porttiin rivillä "http_port 8080". Näin saatiin toimiva konfiguraatio, jolla Squid käynnistyi.

```
auth_param ntlm program c:/squid/libexec/mswin_ntlm_auth.exe
auth_param ntlm children 50

acl all src 0.0.0.0/0.0.0.0
acl whitelist dstdomain "c:\squid\etc\whitelist.txt"
acl koneet src "c:\squid\etc\sallitutkoneet.txt"
acl esimiehet proxy_auth "c:\squid\etc\esimiehet.txt"
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl SSL_ports port 443
acl ftp proto FTP
acl CONNECT method CONNECT

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
```

```
http_access allow ftp
http_access allow whitelist
http_access allow koneet
http_access allow kayttajat
http_access deny all

logformat squid %tl.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log c:/squid/var/logs/access.log squid

http_port 8080
```

Luodaan vielä seuraavat tekstitiedostot:

- c:\squid\etc\whitelist.txt
- c:\squid\etc\sallitutkoneet.txt
- c:\squid\etc\esimiehet.txt

Tekstitiedostojen sisällön muodon määrää pääsylistan tyyppi. Sallittujen sivujen pääsylistan tyyppi on "dstdomain", joten sallittu sivusto laitetaan muodossa ".sivusto.com", ja kun sivustoja on useampia, ne erotetaan rivinvaihdolla.

Sallittujen koneiden lista on tyyppi "src", joten tekstitiedostoon määritetään sallittujen tietokoneiden IP-osoitteet ja ne erotetaan toisistaan rivinvaihdolla.

Esimiesten ja IT-henkilöiden listaan lisättävät henkilöt on laitettava muotoon "toimialue\käyttäjä", ja ne erotetaan rivinvaihdolla.

3.1.7 Keskitetty pääsylistojen hallinta

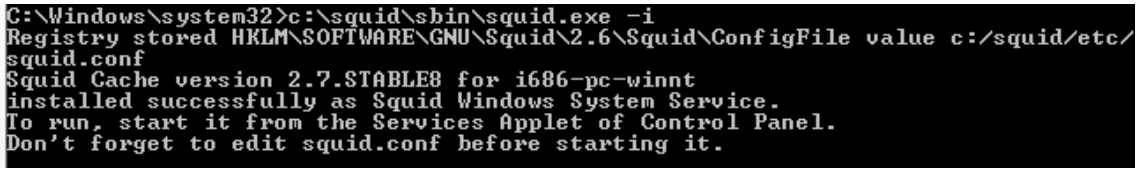
Tähän mennessä oli rakennettu toimiva Squid-välityspalvelin, joka täyttää jo annetut vaatimukset keskitettyä hallintaa lukuun ottamatta. Palvelupisteitä on ympäri Pohjoismaita, ja ne on liitetty samaan verkkoon MPLS- sekä VPN- tekniikoita käyttäen. Olisin voinut ottaa käyttöön pelkästään yhden Squid-palvelimen ja ohjata kaikkien asiakas-

palvelukoneiden liikenteen siihen, mutta tämä olisi aiheuttanut paljon muita ongelmia. Niitä olisi ollut esimerkiksi erittäin suuret vasteajat, koska etäisyydet ovat pitkät sekä VPN-tunnelin tai verkko-ongelman sattuessa koko palvelupisteiden HTTP-liikenne olisi pois käytöstä.

Squid-välityspalvelimen asennus nykyisellä konfiguraatiolla moneen palvelimeen olisi tarkoittanut sitä, että kun pääsylistoihin olisi pitänyt tehdä muutoksia, tulisi käydä ne lisäämässä kaikkien välityspalvelinten pääsylistoihin yksitellen. Ratkaisuna tähän oli asettaa pääsylistojen tekstitiedostot verkkolevylle paikallisen kiintolevyn sijasta. Pääsylistat siirrettiin verkkokansioon ja muutos tehtiin nykyiseen konfiguraatioon.

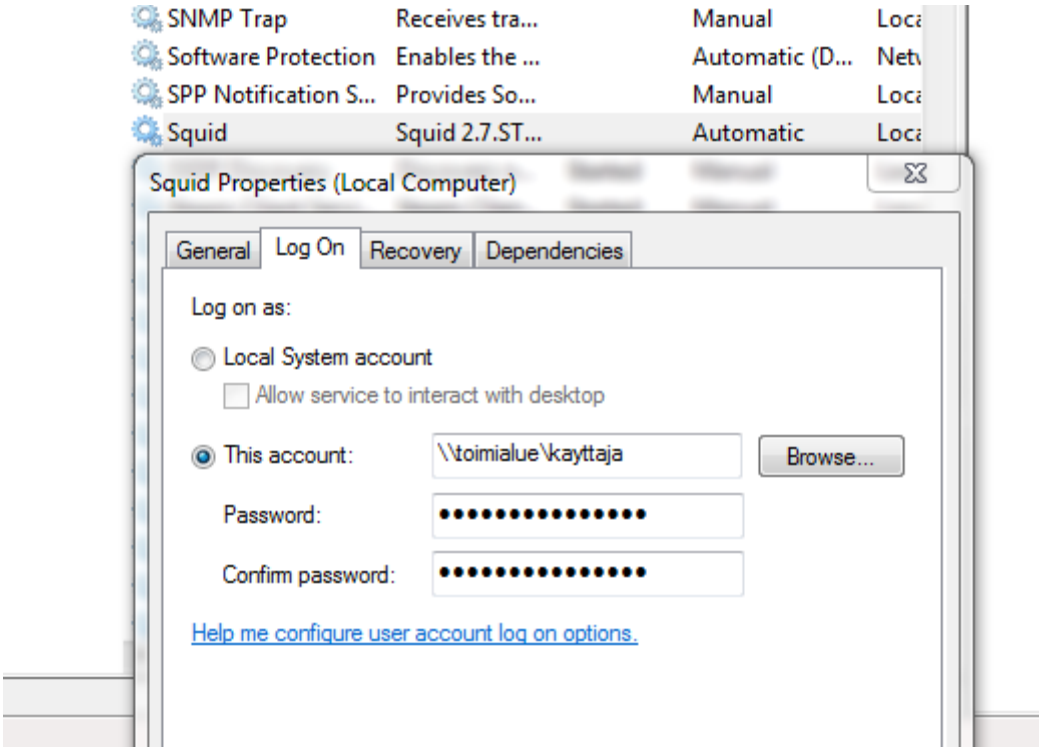
```
acl whitelist dstdomain "\\tiedostopalvelin\it\proxy\whitelist.txt"
acl koneet src "\\tiedostopalvelin\it\proxy\sallitutkoneet.txt"
acl esimiehet proxy_auth "\\tiedostopalvelin\it\proxy\esimiehet.txt"
```

Tästä kuitenkin ilmeni ongelma, kun Squid käynnistettiin, se ajettiin paikallisella järjestelmätilillä, jolla ei ole lukuoikeuksia verkkokansioihin. Ratkaisuna tähän ajettiin Squid komentoriviltä "-i" -parametrilla, joka asentaa Squidin Windows Serviceksi eli taustalla ajettavaksi palveluksi (ks. kuva 7).



Kuva 7. Squidin asennus Windows Serviceksi.

Tämän jälkeen mentiin Windows Service -hallintapaneeliin ja muutettiin Squid-palvelun käyttämään toimialueessa olevaa käyttäjää, jolla on lukuoikeudet verkkokansioon, johon pääsylistat on sijoitettu. Tähän on suositeltavaa asettaa jokin hallintaan tarkoitettu käyttäjätunnus, eli ei siis omaa käyttäjätunnusta (ks. kuva 8).



Kuva 8. Squid-palvelun käynnistyminen määritetyllä käyttäjällä.

Squid oli nyt asennettu Windows Serviceksi ja se oli määritetty käynnistymään käyttäjällä, jolla on lukuoikeudet verkkokansioon, johon pääsylistat on siirretty.

Aina kun pääsylistaa päivitetään, on Squid joko käynnistettävä uudelleen tai sille annettava "-k reconfigure" -käsky, jotta uusi pääsylistan sisältö tulisi voimaan. Pääsylistaa tulisi kuitenkin pystyä päivittämään etänä. Tämä tarkoittaa sitä, että pitäisi olla mahdollista pystyä ajamaan "c:\squid\sbin\squid.exe -n squid -k reconfigure" -komento palvelimeen, johon Squid on asennettu. Tämä komento käskee squid-nimistä prosessia tai palvelua lataamaan uudelleen sen asetukset, jolloin myös pääsylistat päivittyvät. Jotta paikallisen komennon ajaminen onnistuisi etänä toiselta tietokoneelta, tarvittiin siihen apuohjelmaa nimeltä PsExec. Se on osa Microsoftin Sysinternals -työkalupakkia ja sen voi ladata Microsoftin Technet-sivustolta. [9.]

PsExec-apuohjelma toimii pitkälti samalla tavalla kuin esimerkiksi Telnet -yhteys. PsExec kuitenkin mahdollistaa hyvin yksinkertaisella tavalla suorittaa komentoja etätietokoneesta ja jopa käyttämään etätietokoneen komentokehotetta reaaliajassa. PsExec:in vahvoja puolia on myös se, että sitä ei tarvitse asentaa etätietokoneeseen, johon halutaan yhteys ottaa. Seuraavaksi hyödynnettiin PsExec-työkalua ja luotiin ajettavan tie-

dosto, jonka suorittamalla pystyttiin etänä käskeä Squidia ottamaan uudet asetukset ja pääsylistat voimaan. [9.]

Seuraavaksi siirrettiin "\\tiedostopalvelin\it\proxy\" -verkkokansioon PsExec.exe -tiedosto ja luotiin ".bat" -päätteinen tiedosto, jonka sisälle kirjoitettiin komennot, joilla testikoneen Squidin päivitys onnistui.

```
PSEXEC \\testikone c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimi-
alue\kayttaja
```

Tiedoston tallennettiin ja nimettiin nimellä "updateproxy.bat". Kun tämä tiedosto suoritetaan, kohdekoneen Squid ottaa uudet asetukset ja pääsylistat käyttöön. Komennossa "-n" -parametri määrittää tämän komennon koskemaan "squid"- nimistä Windows Serviceä, "-k reconfigure" antaa käskyn päivittää asetustiedostot ja pääsylistat."-u" -komennolla määritetään käyttäjätili, jolla on oikeus ajaa komento etätietokoneeseen. Tähän kannattaa asettaa sama käyttäjätili, jolla on Squid-palvelu käynnistetty (ks. kuva 8).

3.1.8 Testaus tuotantoympäristössä

Edellisessä luvussa tehtiin mahdolliseksi päivittää Squid-välityspalvelimen asetukset ja pääsylistat suorittamalla verkkokansiosta "updateproxy.bat" tiedoston. Tämä tarkoitti sitä, että Squidiin pystyttiin päivittämään uudet pääsylistat miltä koneelta tahansa ajamalla "updateproxy.bat" tiedoston.

Ennen kuin Squid asennettiin ja otettiin käyttöön kaikissa asiakaspalvelupisteissä, teimme viikon kokeiluajanjakson yhdessä asiakaspalvelupisteessä. Tarkoituksena oli saada esille ilmeneviä ongelmia Squidin konfiguraatiossa sekä toiminnassa ja korjata ne ennen kuin Squid otettiin laajempaan käyttöön.

Squid asennettiin asiakaspalvelupisteen palvelimelle ja testikoneesta kopioitiin konfiguraation siihen. Tämän jälkeen välityspalvelin otettiin käyttöön asiakaspalvelukoneissa samalla tavalla Internet Explorerin asetuksista kuin se otettiin testikoneessakin (ks. kuva 4). Tässä asiakaspalvelupisteessä työskentelevät esimiehet lisättiin "\\tiedostopalvelin\it\proxy\esimiehet.txt" -tiedostoon, toimistokoneen IP-osoitteen "\\tiedostopalvelin\it\proxy\sallitutkoneet.txt" -tiedostoon ja lopuksi tehtiin muutokset

"\\tiedostopalvelin\it\proxy\updateproxy.bat" -tiedostoon. Myös "updateproxy.bat" tiedostosta muutettiin "\\testikone" -kohdan osoittamaan asiakaspalvelupisteen palvelinta, johon Squid on asennettu.

Viikon kokeilujakson aikana ilmeni seuraavanlaiset ongelmat:

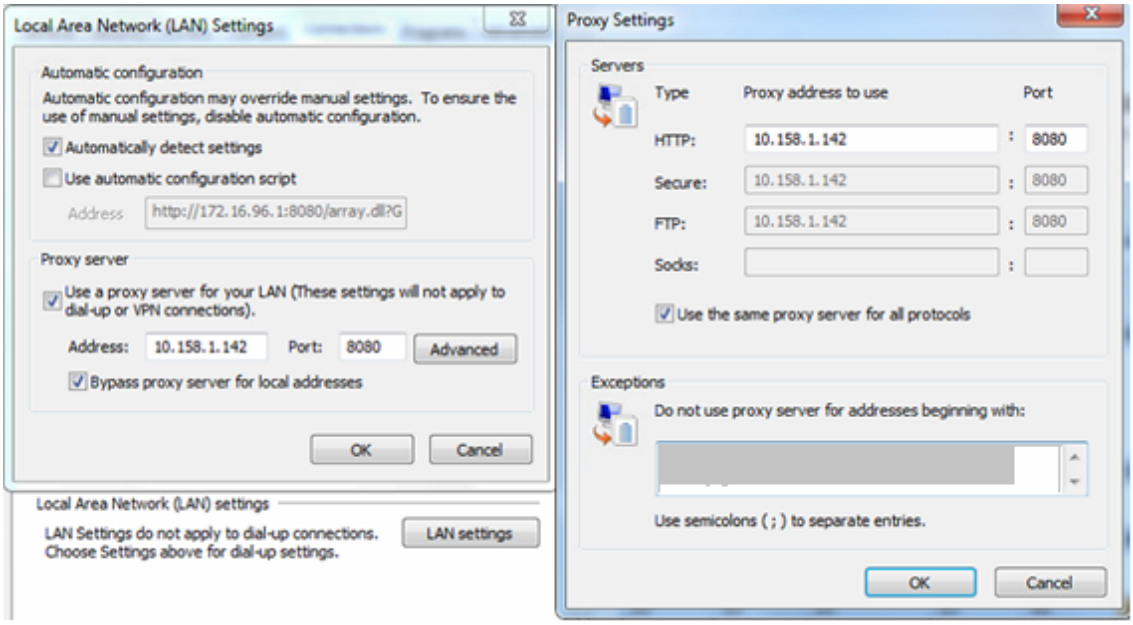
- Sivustot eivät näkyneet oikealla tavalla tai niistä puuttui sisältöä.
- Työntekijät eivät päässeet kaikille HTTPS-sivustoille.
- Osa työntekijöiden käyttämistä ohjelmista lakkasi toimimasta.
- Osa Intranetin palveluista lakkasi toimimasta.

Ongelmien selvittämisessä access.log -lokitiedosto on erittäin tärkeä. Sitä tutkimalla pystyttiin selvittämään, mistä ongelmat johtuivat. Kaikki sivustot eivät näkyneet kunnolla, koska niiden sisällä saattoi olla sisältöä toisilta sivustoilta, joita ei oltu sallittu. Esimerkiksi säätiedotus-sivusto saattaa hakea itse säätiedot toiselta sivustolta tai uutissivusto käyttää toisen uutissivuston sisältöä. Ongelmat pystyttiin korjaamaan katsomalla access.log -tiedostosta, mihin kaikkiin sivustoihin on yritetty ottaa yhteyttä ja mitkä niistä estetty.

Useat HTTPS-sivustot eli salausta käyttävät sivustot lopettivat toimintansa. Tämä johtui siitä, että konfiguraatiossa oli sallittu SSL/TLS -liikenteelle ainoastaan oletusportti eli portti 443. Yrityksessä kuitenkin käytetään paljon sivustoja, jotka eivät käytä tätä oletusporttia. Tämän takia Squid-konfiguraatiossa muutettiin riviä "acl SSL_ports port 443" ja "443":n tilalle tuli laittaa "1-65535". Tällöin Squid päästää läpi kaiken HTTPS-liikenteen kaikista porteista.

Osa työntekijöiden käyttämistä ohjelmista käyttävät tiedonsiirrossa HTTP-liikennettä. Ongelmaksi ilmeni, että nämä ohjelmat lähettävät HTTP-pyynnöt HTTP-tunnisteella "Expect: 100-continue". Tätä tunnistetta käytetään silloin, kun ohjelma ilmoittaa palvelimelle, että se olisi lähettämässä tietoa, ja jää odottamaan hyväksyntää palvelimelta. Squidin versio 2.7 ei kuitenkaan tue tätä tunnistetta eikä se siksi päästä kyseistä tunnistetta läpi. Squidin konfiguraation alkuun voidaan kuitenkin lisätä rivi "ignore_expect_100 on", joka jättää Squidin huomioimatta "Expect: 100-continue" -tunnisteet ja päästää ne läpi. [8.]

Viimeisenä ongelmana oli se, että osa intranetin palveluista lakkasi toimimasta. Esimerkiksi intranet-sivustolla toimiva työkalu, jonka avulla haetaan asiakkaasta tietoa tietokannasta, ei toiminut. Ongelmaan ei löytynyt varsinaisesti mitään korjausta, joten helpoin tapa saada nämä toimimaan oli katsoa access.log:sta, mihin intranet-palvelimeen tietokone yritti ottaa yhteyttä, kun tietokantahakua tehtiin, ja lisätä palvelimen osoite Internet Explorerin asetuksissa olevaan listaan, jossa on sivustot joita ei lähetetä välityspalvelimelle (ks. kuva 9).



Kuva 9. Intranet-palvelimet lisättynä Exceptions -listaan.

Tämän kokeilujakson aikana sallittujen sivustojen listaan lisättiin paljon uusia sivustoja, joita käytetään työnteossa. Usein työntekijä ilmoittaa esimiehelle tietystä sivustosta ja kertoo, että mihin sitä käytetään, jonka jälkeen esimies ottaa yhteyttä IT:hen ja IT sitten lisää sivuston sallittujen sivujen joukkoon.

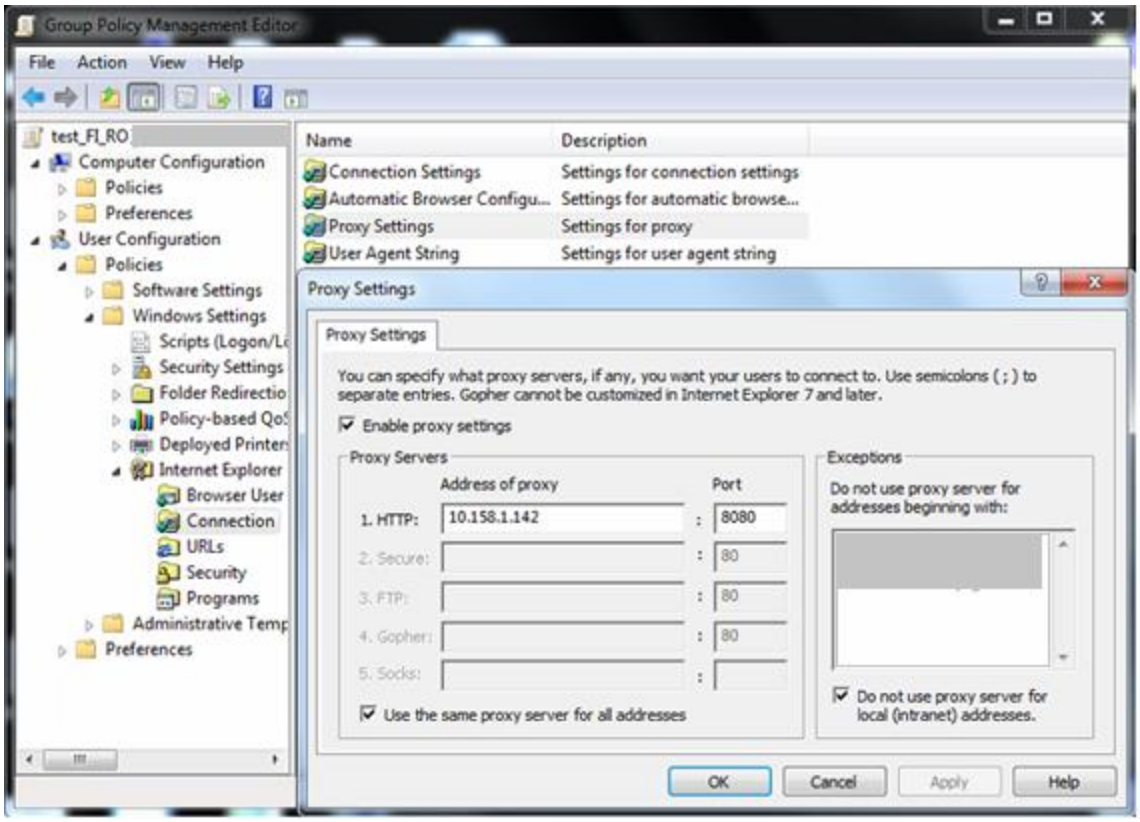
3.2 Välityspalvelimen laajempi käyttöönotto

Viikon testijakson ja ongelmien korjauksien jälkeen oli aika asentaa ja ottaa välityspalvelin käyttöön kaikkiin palvelupisteisiin. Palvelupisteissä käytettiin korjattua konfiguraatiota ja muutamien palvelupisteiden konfiguraatiosta kommentoimme rivit, jotka määrittävät uudelleenohjauksen seuraavalle välityspalvelimille [liite 1]. Näissä palvelupisteissä ei ollut tarvetta ohjata liikennettä seuraavalle välityspalvelimelle.

Squid asennettiin kaikkiin palvelupisteisiin korjatulla konfiguraatiolla ja tämän jälkeen syötettiin kaikkien muidenkin palvelupisteiden esimiehet sekä toimistokoneet pääsylistoihin. "updateproxy.bat" -tiedostoon lisättiin vielä kaikkien asiakaspalvelupisteiden Squid-välityspalvelimien konfiguraation uudelleenlataamiskomennon. Kun "updateproxy.bat" ajetaan läpi, päivittyvät uudet pääsylistat kaikkiin palvelupisteisiin samalla kertaa.

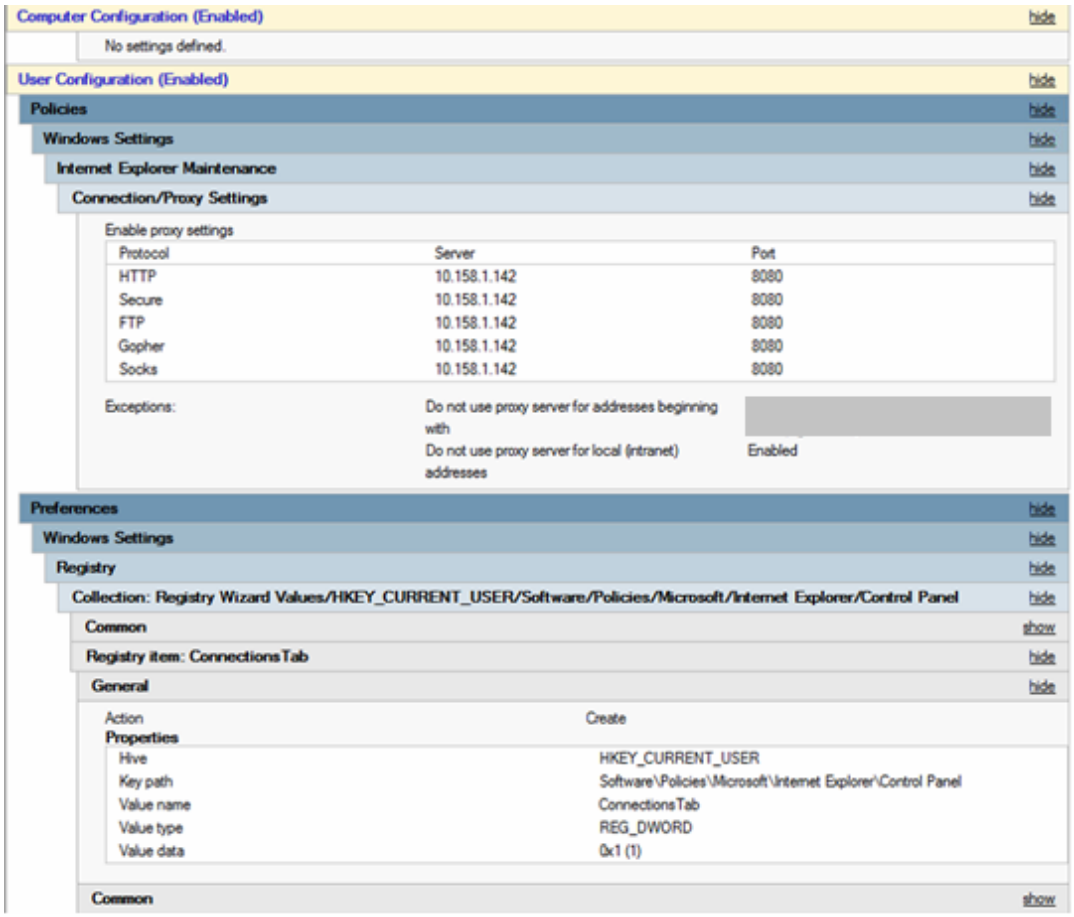
```
PSEXEC \\palvelin1 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
PSEXEC \\palvelin2 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
PSEXEC \\palvelin3 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
PSEXEC \\palvelin4 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
PSEXEC \\palvelin5 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
PSEXEC \\palvelin6 c:\squid\sbin\squid.exe -n squid -k reconfigure -u toimialue\kayttaja
```

Lopuksi hyödynnettiin ryhmäkäytäntöjä ja käyttäjiltä piilotettiin Internet Explorerin asetuksista Connection-välilehti, sekä määritetään kaikkien palvelupisteiden tietokoneet ottamaan käyttöön niille tarkoitetun Squid-välityspalvelimen. Koska kaikki palvelupisteet ovat omassa organisaatioyksikössä (OU) aktiivihakemistossa, pystyttiin helposti luomaan palvelupistekohtaiset ryhmäkäytännöt ja ottamaan käyttäjille käyttöön niille kuuluvan välityspalvelimen. Seuraavaksi luotiin jokaiselle palvelupisteelle oma GPO:n (Group Policy Object) ja määritettiin jokaiselle palvelupisteelle oma Squid välityspalvelin osoite käyttöön (ks. kuva 10). Käyttäjien tietokoneiden rekisteriin luotiin "Software\Policies\Microsoft\Internet Explorer\Control Panel\ConnectionsTab" -rekisteriavain, jonka arvoksi asetettiin "1". Tämä rekisteriavain piilottaa käyttäjiltä Connection-välilehden Internet Explorerin asetuksista.



Kuva 10. Välityspalvelimen määritys ryhmäkäytäntöön.

Kuvassa 11 näkyy luotu ryhmäkäytäntö, jossa otettiin välityspalvelin käyttöön, sekä rekisteriavain, joka piilottaa Connection-välilehden Internet Explorerin asetuksista. Jokaiselle asiakaspalvelupisteen organisaatioyksikölle luotiin oma ryhmäkäytäntö, koska jokaiselle niistä oli määritettävä paikallisen Squid-välityspalvelimen osoite.



Kuva 11. Valmis ryhmäkäytäntö tarvittavilla muutoksilla.

3.3 Työ käyttöönoton jälkeen

Välityspalvelimet otettiin käyttöön kaikissa asiakaspalvelupisteissä elokuussa 2012, ja koska työ on todettu toimivaksi ratkaisuksi, on siitä pidetty kiinni. Pääsylistoja, esimieslistoja ja sallittujen tietokoneiden listaa päivitetään jatkuvasti. Joitakin ongelmia on esiintynyt käyttöönoton jälkeen, niistä osa on jo korjattu tavalla tai toisella. Jotkut ei niin kriittiset ongelmat odottavat vielä korjausta. Esimerkiksi osassa asiakaspalvelupisteissä saattaa satunnaisesti tulla sähkökatkoksia, ja vaikka palvelin, jossa välityspalvelin sijaitsee, käynnistyy automaattisesti uudelleen, Squid palvelu pitää manuaalisesti uudelleen käynnistää.

On tullut huomattua, että access.log lokitiedosto on erittäin tärkeä selvittäessä, miksi sivusto ei toimi kunnolla. Useat sivustot sisältävät sisältöä myös muista sivustoista ja täten ne on myös sallittava, jotta sivustokokonaisuus toimisi suunnitellusti. Lokitiedos-

tosta selviää, mihin muualle sivustoa avattaessa on yritetty ottaa yhteyttä ja tämän kokonaisuuden voi sitten lisätä sallittujen sivujen listalle. Toisaalta myös mainokset jäävät sivustoilta pois, koska yleensä mainokset tulevat mainostajan sivustoilta, joita ei ole sallittu eikä niitä täten näytetä.

Suurin syy tietokoneiden saastumiselle oli, että vanhalla verkkoselaimella käydään sivustolla, joka hyödyntää verkkoselaimesta löytyviä tietoturva-aukkoja. Eston ansiosta virushälytykset ovat kadonneet kokonaan asiakaspalvelupisteiden tietokoneista.

4 Yhteenveto

Tässä työssä toteutettiin helposti ylläpidettävä välityspalvelin, jonka tarkoituksena oli rajoittaa asiakaspalvelupisteissä käytettävien tietokoneiden internetin käyttöä vain sallittuihin sivustoihin. Squid-niminen välityspalvelinohjelmisto valittiin käytettäväksi, ja se osoittautui toimivaksi ratkaisuksi.

Aihe oli itselleni täysin vieras, ja siksi aikaa kului paljon niin toteutuksen miettimiseen kuin myös sen toteuttamiseen. Haastavaa oli saada tehtyä toimiva konfiguraatio sekä vianetsintä. Moni intranet-sivusto ja ohjelma lakkasi toimimasta Squidin käyttöönoton jälkeen, ja niiden vianetsintä kulutti paljon aikaa.

Työ täytti kaikki asetetut tavoitteet. Sallittujen sivustojen lisääminen ja ylläpitäminen on tehty helpoksi ja nopeaksi, koska uusi sallittu sivusto tarvitsee vain lisätä yhteen tekstitiedostoon, joka päivittyy kaikille asiakaspalvelupisteille. Myös esimiehille ja sallituille tietokoneille on omat listansa. Hyvinä puolia on myös huomattu mainosten häviäminen, tietokoneita saastuttavien viruksien häviäminen sekä nopeammin latautuvat sivustot. Haittapuolia ei tullut vastaan. Välityspalvelimet ovat käytössä yrityksen kaikissa asiakaspalvelupisteissä, ja ne tullaan myös ottamaan käyttöön tulevissa asiakaspalvelupisteissä.

Lähteet

1 Squid: Optimising Web Delivery2012. Squid-cache.org. Verkkodokumentti. <http://squid-cache.org>. Luettu 12.6.2012.

2 Privoxy - Home Page. 2012. Verkkodokumentti. Privoxy Developers. <http://www.privoxy.org/>. Luettu 12.6.2012.

3 Squid-cache wiki. 2012. Verkkodokumentti. Squid-cache.org. <wiki.squid-cache.org/>. Luettu 12.6.2012.

4 Squid for Windows. Verkkodokumentti. Acme Consulting. <http://squid.acmeconsulting.it>. Luettu 12.6.2012.

5 Squid: A User's Guide. 2012. Verkkodokumentti. Huihoo. <http://docs.huihoo.com/gnu_linux/squid/html/x1793.html>. Luettu 18.6.2012.

6 Squid, Uses of ACLs. 2012. Verkkodokumentti. Oskar Pearson. <http://www.deckle.co.uk/squid-users-guide/squid-access-control-and-access-control-operators.html>. Luettu 18.6.2012.

7 Squid glossary. 2012. Verkkodokumentti. ViSolve. <http://www.visolve.com/squid/squid24s1/glossary.php >. Luettu 26.6.2012.

8 Squid Expect: 100-continue header issues. 2012. Verkkodokumentti. WordPress.com. <http://alpacapowered.wordpress.com/2012/06/21/squid-expect-100-continue-header-issues/> Luettu 7.8.2012.

9 Windows Sysinternals, PsExec. 2009. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>. Luettu 4.7.2012.

10 Elisa Oyj Pressi tiedotteet. 2012. Verkkodokumentti. Elisa Oyj. <https://www.elisa.fi/ir/pressi/index.cfm?t=100&o=5130&did=17727>. Luettu 2.5.2013.

11 TeliaSonera uutishuone. 2012. Verkkodokumentti. TeliaSonera. <http://uutishuone.sonera.fi/media/2012/07/30/sonera-toteutti-pirate-bay--estot/598baa16-a6c9-4660-855c-27e22a11fb7c>. Luettu 2.5.2013.

12 Microsoft Windows Family Safety. 2013. Verkkodokumentti. Microsoft. <http://windows.microsoft.com/fi-fi/windows7/protecting-your-kids-with-family-safety>. Luettu 2.5.2013.

Lopullinen konfiguraatio

```
#Authentikoinnin määrittely

auth_param ntlm program c:/squid/libexec/mswin_ntlm_auth.exe

auth_param ntlm children 20


#"All" pääsylista

acl all src 0.0.0.0/0.0.0.0


#Sisältää listan sallituista verkkotunnuksista

acl whitelist dstdomain "\\tiedostopalvelin\it\proxy\whitelist.txt"

#Sisältää listan sallituista tietokoneista

acl koneet src "\\tiedostopalvelin\it\proxy\sallitutkoneet.txt"

#Sisältää sallitut käyttäjät (esimiehet, IT)

acl esimiehet proxy_auth "\\tiedostopalvelin\it\proxy\esimiehet.txt"


#Sisältää avoimet portit

acl Safe_ports port 80 81 21 443 563 70 210 1025-65535

acl SSL_ports port 1-65535


#Sisältää FTP liikenteen
```

```
acl ftp proto FTP


#Käytetään tunnelointiin
acl CONNECT method CONNECT


#Estetään kaikki portit jotka eivät ole Safe_ports listassa
http_access deny !Safe_ports
#Tunneloidaan SSL liikenteen
http_access deny CONNECT !SSL_ports
#Sallitaan FTP liikenne
http_access allow ftp
#Sallitaan pääsylistojen sisältöjä
http_access allow whitelist
http_access allow koneet
http_access allow kayttajat
#Estetään kaikki liikenne
http_access deny all


#Liikenteen ohjaus seuraavalle välityspalvelimelle. Käytetään vain jos tarvetta.
cache_peer 172.16.5.1 parent 8080 0 no-query no-digest
never_direct allow all
```

#Luodaan squid lokiformaatti ja asetetaan sen access lokin käyttöön.

logformat squid %tl.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt

access_log c:/squid/var/logs/access.log squid

#Asetetaan Squid kuuntelemaan porttia 8080

http_port 8080